UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,625	02/13/2002	Victor Tang	51373-113	7343

59555 7590 10/25/2006

RATHE PATENT & IP LAW
10611 W. HAWTHORNE FARMS LANE
MEQUON, WI 53097

EXAMINER	
PATEL, CHIRAG R	

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 10/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/074,625	TANG ET AL.	
	Examiner	Art Unit	
	Chirag R. Patel	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments filed August 15, 2006 have been fully considered but they are not persuasive. A discussion is provided below.

Kadyk discloses per [0060], "The step for authenticating a user may include HTTP basic authentication, HTTP digest authentication, or some other type of authentication, such as authentication based on a client certificate that is exchanged at the time a secure client-proxy connection is established." Basic authentication reads on claim limitations "plain text unencrypted information". Digest reads on claim limitations "obscured user name".

Kadyk discloses per [0062], "As noted with respect to FIG. 4, by encapsulating the secure end-to-end connection within the insecure client-proxy connection, the overhead associated with establishing a separate connection is avoided. Furthermore, because the *insecure client-proxy connection does not perform any encryption*, the overhead of encapsulating the secure end-to-end connection within the insecure client-proxy connection is minimal." The communication between client and proxy is insecure.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Kadyk et al. – hereinafter Kadyk – (US 2002/0157019)

As per claim 1, Kadyk discloses a method of protecting a username during authentication, the method comprising:

obtaining a plain text username over a secure communication channel; obtaining a server identifier for a server; ([0045]; basic authorization supports limitation of plain text username; [0049]; the sockets layer ("SSL") connection meets the limitation for the "secure communication channel", Figure 2 item 230; act of obtaining a plain text username, [0049]; Figure 3A: item 330)

obscuring the plain text username using the server identifier; ([0007], [0045]; digest authorization hashes the user name)

providing the obscured username and the plain text username to the server; and ([0045], Figure 2B-1: items 224b, 226b)

communicating authentication information including plain text unencrypted information and the obscured username over a non-secure communication channel from a client. ([0012]-[0013], [0060]-[0062] Reference 550 finally shows a step for encapsulating the secure end-to-end connection within the now insecure client-proxy connection.)

As per claim 2, Kaydk discloses the method of claim 1 wherein the server identifier is a uniform resource locator (URL) corresponding to the server. ([0053]; http – hypertext transfer protocol refers to a URL; uniform resource locater)

As per claim 3, Kaydk discloses the method of claim 1, wherein the server identifier is an authentication domain corresponding to the server. ([0047];)

As per claim 4, Kaydk discloses the method of claim 1, wherein obscuring the plain text username using the server identifier comprises encrypting the plain text username using an encryption method. ([0045; digest authorization hashes the user name)

As per claim 5, Kaydk discloses the method of claim 17 wherein the encryption method is advanced encryption standard (AES). ([0045; digest authorization is an advanced encryption standard)

As per claim 6, Kaydk discloses the method of claim 1, wherein the client is a wireless device. ([0043]; wireless link)

As per claim 7, Kaydk discloses the method of claim 1, wherein obtaining a plain text username over a secure communication channel comprises establishing an encrypted communication session between the user and the server and communicating

a plain text username from the user to the server. ([0035]; basic authorization supports plain text username)

As per claim 8, Kaydk discloses the method of claim 1, wherein the authentication information satisfies a plain text, unencrypted authentication scheme. ([0045; basic authorization meets the limitations of plain text, unencrypted authentication scheme)

As per claim 9, Kaydk discloses the method of claim 1, wherein the server identifier is a combination of an authentication domain and a uniform resource locator (URL) of the server. ([0047]; ([0053]; http – hypertext transfer protocol refers to a URL; uniform resource locater)

As per claim 10, Kaydk discloses a username protection process comprising:

registering a user with a selected server by requesting and receiving a plain text user identifier, creating an obscure version of the plain text user identifier, and storing the plain text user identifier and the obscure version of the plain text user identifier on the selected server; and ([0040], [0045]; basic authorization supports limitation of plain text username, Figure 2 item 230; act of obtaining a plain text username)

initiating a communication session between the user and the selected server by the communication of the obscure version of the plain text user identifier and plain text unencrypted information over a plain text communication channel. ([0012-0013], [0060]-

[0062]; finally, reference 550 shows a step for encapsulating the secure end-to-end connection within the now insecure client-proxy connection.)

As per claim 11, Kaydk discloses the process of claim 10, wherein the user is a wireless client device communicating over a non-encrypted channel. ([0043]; wireless link)

As per claim 12, Kaydk discloses the process of claim 10, wherein communication over a plain text channel involves the obscure version of the plain text user identifier and communication over a secure channel can use the plain text user identifier. ([0045]; digest authorization hashes the user name as far as the limitation of the obscure version o f the plain text user identifier, [0061]; finally, reference 550 shows a step for encapsulating the secure end-to-end connection within the now insecure client-proxy connection.)

As per claim 13, Kaydk discloses the process of claim 10, wherein the obscure version of the plain text user identifier is stored on the user device. ([0040], [0045]; digest authorization hashes the user name)

As per claim 14, Kaydk discloses a system for protecting a username during authentication over a non-encrypted channel, system comprising:

a client device being configured to communicate plain text unencrypted information over unsecure communication channels using an obscured user identifier; and ([0053]-[0056]; [0060]-[0062]; Figure 4: item 402)

a server having stored therein a plain text user identifier communicated by the client device over a secure communication channel and an obscured user identifier corresponding to the plain text user identifier. ([0053]-[0056]; Figure 4: item 406)

As per claim 15, Kaydk discloses the system of claim 14, further comprising a registration device being configured to communicate information over secure communication channels. ([0053]-[0056]; Figure 4: item 404)

As per claim 16, Kaydk discloses the system of claim 15, wherein the client device and registration device are the same device. ([0027])

As per claim 17, Kaydk discloses the system of claim 14, wherein the client device does not encrypt communication when communicating with the obscured user identifier created from the plain text user identifier. ([0045]; basic authorization does not encrypt communication, [(0053)-(0056)])

As per claim 18, Kaydk discloses the system of claim 14, wherein the client device has stored therein the plain text user identifier and the obscured user identifier. ([0040],[0045])

As per claim 19, Kaydk discloses the system of claim 14, wherein the obscured user identifier corresponding to the plain text user identifier is created by encrypting the plain text user identifier with a key. ([0045]; digest authorization hashes the user name, [0050])

As per claim 20, Kaydk discloses the system of claim 19, wherein the key is based on the uniform resource locator (URL) of the server or an authentication domain of the server. ([0047]; ([0053]; http – hypertext transfer protocol refers to a URL; uniform resource locater)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag R. Patel whose telephone number is (571)272-7966. The examiner can normally be reached on Monday to Friday from 7:30AM to 4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia, can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pairdirect.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER